Alex R. Straus, SBN 321366
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
(917) 471-1894 (phone)
(615) 921-6501 (fax)
astraus@milberg.com

Plaintiffs' Attorneys

Additional attorneys on signature page

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

VICKEY ANGULO, individually and on behalf of themselves and all others similarly situated, Plaintiffs, v. SUPERCARE HEALTH, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **Demand for Jury Trial**

Plaintiff Vickey Angulo ("Plaintiff") brings this Complaint against Defendant SuperCare Health, Inc. ("SCH"), individually and on behalf of all others similarly situated, and alleges upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. On or about March 25, 2022, SCH posted a notice, entitled Notice of Data Breach (hereinafter, the "Notice"), announcing publicly that an unauthorized actor accessed SCH's files.

2. According to SCH's Notice, current and former patients' personally identifiable information ("PII") and protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including, but not limited to, patients' names, addresses, dates of birth, hospital or medical group, patient account numbers, medical record numbers, health insurance information, testing/diagnostic/treatment information, and other health-related information, as well as, for some, Social Security numbers and driver's license numbers (collectively, the "Private Information"), were accessed and compromised by an unauthorized third party in the cybersecurity incident (the "Data Breach").

3. As detailed below, the Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and the Class Members' Private Information despite the fact that data breach attacks against medical systems and healthcare providers are at an all-time high.

4. This attack enabled an unauthorized third-party to access SCH's computer systems and the highly sensitive and confidential data of thousands of current and former patients of SCH, including Plaintiff.

5. Plaintiff received a notification letter from SCH informing her that the information accessed by the third-party actors included her electronic health records.

6. SCH, despite professing to take the privacy and security of its patients' confidential and health information seriously, has not offered to provide affected individuals with adequate credit monitoring service or compensation for the damages they have suffered as a result of the Breach.

7. As a consequence of the Data Breach, Plaintiff's and Class members' Private Information has been released into the public domain and they have had to, and will continue to have to, spend time to protect themselves from fraud and identity theft.

8. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, through frequent news reports and FBI warnings to the healthcare industry, and thus it was on notice that failing to take steps necessary to secure the Private Information from those risks left the property in a dangerous and vulnerable condition.

9. Defendant disregarded the rights of Plaintiff's and Class Members (defined below) by, inter alia, intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach and failing to provide Plaintiff and Class Members accurate notice of the Data Breach.

10. Plaintiff's and Class Members' identities are now at risk because of Defendant's conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class

Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and/or giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

14. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

II. JURISDICTION AND VENUE

16. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant to establish minimal diversity.

17. The Central District of California has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and conducts substantial business in California and this District through its headquarters, offices, and affiliates.

18. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and has caused harm to Plaintiff and Class Members residing in this District.

III. PARTIES

19. Plaintiff Vickey Angulo is a resident and citizen of the State of California and intends to remain domiciled in and a citizen of the State of California. Plaintiff received Notice of the Data Breach on or about March 25, 2022. She was informed the following sensitive data she provided to SCH was compromised in the Data Breach:

name, address, date of birth, patient account number, diagnostic information, and claim information.

20. Defendant SuperCare Health, Inc. is a respiratory health company that is headquartered at 8345 Firestone Blvd., Suite 210, Downey, California 90241.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

21. According to Defendant's website, "SuperCare Health is the leading post-acute, in-home respiratory care provider in the western U.S. that has been serving the healthcare needs of our ever-growing patient population for nearly 50 years."

22. As part of promoting its business, Defendant boasts "[consumer] privacy is important to [SuperCare Health]."

23. Pursuant to Defendant's Privacy Policy, it collects the following sensitive information from consumers:

a. Name

b. Date of Birth

c. SuperCare Health Account ID

d. Medical diagnosis

e. Home or work address

f. Telephone number

g. Zip code

h. Age

i. Gender

24. On information and belief, and, as indicated in Defendant's Notice of Data Breach, Defendant also collects Social Security numbers and driver's license numbers – which were compromised for a number of victims of the Data Breach.

25. In the ordinary course of transacting with Defendant, consumers are required to provide – and Plaintiff did so provide – Defendant with extremely sensitive and personal PII and PHI.

26. Additionally, Defendant may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends and/or family members.

27. As current and former patients at SCH, Plaintiff and Class members relied on SDCA to keep their highly sensitive information confidential and securely maintained.

28. On information and belief, Defendant provides each of its patients, including Plaintiff, with a HIPAA compliant notice of its privacy practices (the "Privacy Notice") in respect to how it handles patients' sensitive and confidential information.

29. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, Defendant promises to maintain the confidentiality of patients' health, financial, and non-public personal information, ensure compliance with federal and state laws and regulations, and not to use or disclose patients' health information for any reasons other than those expressly listed in the Privacy Notice without written authorization.

30. As a condition of receiving medical care and treatment from Defendant, Defendant requires that its patients, including Plaintiff and Class Members, entrust it with highly sensitive personal information.

31. Prior to receiving medical care and treatment from Defendant, Plaintiff gave (and was required to give) her highly sensitive Private Information to Defendant.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII and PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII and PHI from unauthorized disclosure.

33. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII and PHI.

34. Plaintiff and the Class members relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE BREACH

35. On or about March 25, 2022, SCH began informing affected individuals, including Plaintiff, that its computer network had been accessed by an unauthorized third party actor by way of a cyberattack and resulting data breach.

36. Although the notification letter states that SCH was the victim of a data security incident on or about July 23, 2021 – July 27, 2021, it provides scant detail about the nature, severity or duration of the attack. Even worse, SCH did not inform their patients of the data breach until over six months after the data breach occurred.

37. But what's clear from the Notice is that cybercriminals did, in fact, access and view Plaintiff's and Class members' PII and PHI during the time period in which the cybercriminals had unfettered access to Defendant's IT network, as that is the modus operandi of cybercriminals who commit such attacks.

38. According to SCH, the attack compromised a wide range of PII and PHI, including but not limited to patients' names, addresses, dates of birth, hospital or medical group, patient account numbers, medical record numbers, health insurance information, testing/diagnostic/treatment information, and other health-related information, as well as, for some, Social Security numbers and driver's license numbers.

39. Simply put, SCH could have prevented this Data Breach.

40. SCH did not implement or maintain adequate measures to protect its patients' PII and PHI.

41. On information and belief, the PII and PHI compromised in the files accessed by hackers was not encrypted.

42. Moreover, the removal of PHI and other PII and PHI from Defendant's system, including, but not limited to, names, dates of birth, Social Security Numbers (which are the keys to identity theft and fraud), and other health information — demonstrates that this cyberattack was targeted due to Defendant's status as a healthcare facility that houses sensitive PII and PHI.

43. Due to Defendant's incompetent security measures, Plaintiff and the Class Members now face a present and substantial risk of fraud and identity theft and must deal with that threat forever.

44. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII and PHI, SCH provided unreasonably deficient protections prior to the Breach, including, but not limited to a lack of security measures for storing and handling patients' PII and PHI and inadequate employee training regarding how to access, handle and safeguard this information.

45. SCH failed to adequately adopt and train its employees on even the most basic of information security protocols, including:

a. storing, locking encrypting and limiting access to patients' highly sensitive PHI;

b. implementing guidelines for accessing, maintaining and communicating sensitive PHI, and

c. protecting patients' sensitive PHI by implementing protocols on how to utilize such information.

46. SCH's failures caused the unpermitted disclosure of Plaintiff's and Class members' Private Information to an unauthorized third party and put Plaintiff and the Class at serious, immediate and continuous risk of identity theft and fraud.

47. The Breach that exposed Plaintiff's and Class members' PHI was caused by SCH's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

48. SCH failed to comply with security standards or to implement security measures that could have prevented or mitigated the Breach.

49. SCH failed to ensure that all personnel with access to its patients' PII and PHI were properly trained in retrieving, handling, using and distributing sensitive information.

THE BREACH WAS FORSEEABLE

50. Defendant had obligations created by HIPAA, contract, industry standards, common law and its own promises and representations made to Plaintiff and Class Members to keep their PII and PHI confidential and to protect it from unauthorized access and disclosure.

51. Plaintiff and Class members provided their PII and PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

52. Defendant's data security obligations were particularly important given the substantial increase in ransomware attacks and/or data breaches in the healthcare industry preceding the date of the breach.

53. Data breaches, including those perpetrated against the healthcare sector of the economy, have become extremely widespread.

54. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.

55. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.

56. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

57. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

58. In 2021 alone there were over 220 data breach incidents.

59. These approximately 220 data breach incidents have impacted nearly 15 million individuals.

60. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

61. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.

62. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

63. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."

64. PII and PHI is of great value to hackers and cybercriminals, and the data compromised in the Breach can be used in a variety of unlawful manners.

65. PII and PHI can be used to distinguish, identify or trace an individual's identity, such as their name, Social Security Number and medical records.

66. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace and mother's maiden name.

67. Given the nature of this Data Breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cybercriminals in a variety of different ways.

68. Indeed, the cybercriminals who possess the Class members' PII and PHI can readily obtain Class members' tax returns or open fraudulent credit card accounts in the Class members' names.

69. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including, upon information and good faith belief, SCH.

DEFENDANT FAILED TO FOLLOW FTC GUIDELINES

70. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

71. According to the FTC, the need for data security should be factored into all business decision-making.

72. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

73. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

74. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

75. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. These FTC enforcement actions include actions against healthcare providers like Defendant. See, e.g., In the Matter of Labmd, Inc., A Corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

78. Defendant failed to properly implement basic data security practices.

79. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

80. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILED TO MEET INDUSTRY STANDARDS

81. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

82. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

83. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

84. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1,

PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

85. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Breach.

DEFENDANT VIOLATES HIPAA AND EVIDENCES INSUFFICIENT DATA SECURITY

86. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

87. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

88. Title II of HIPAA contains what are known as the Administrative Simplification provisions. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI and PII like the data Defendant left unguarded.

89. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D) and 45 C.F.R. § 164.530(b).

> A data breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

90. Data breaches are Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).

91. 91. Defendant's Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

92. Defendant breached its obligations to Plaintiff and the Class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, network and data.

93. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' PHI and other PII and PHI;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

i. Failing to properly train and supervise employees in the proper handling of inbound emails;

j. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

k. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

l. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

m. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

n. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

o. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

p. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

q. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b) and/or

r. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning

> without use of a confidential process or key," 45 CFR § 164.304 (definition of encryption).

94. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and the Class members' PII and PHI.

95. Accordingly, as outlined below, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud and identity theft.

96. In addition, Plaintiff and the Class members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

DATA BREACHES ARE DISRUPTIVE & PUT CONSUMERS AT RISK

97. Hacking incidents and data breaches at medical facilities like Defendant are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

98. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[8]

99. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.

100. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

101. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

102. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

103. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more

information about a victim's identity, such as a person's login credentials or Social Security number.

104. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

105. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

106. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

107. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may

obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

108. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:

109. Moreover, theft of PII and PHI is also gravely serious. PII and PHI is an extremely valuable property right.

110. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII and PHI has considerable market value.

111. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

112. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies

of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

113. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when PII, PHI, and/or financial information is stolen and when it is used.

114. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. See GAO Report, at p. 29.

115. PII and PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

116. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

117. Thus, Plaintiff and Class members must vigilantly monitor their financial and medical accounts for many years to come.

118. Sensitive PII and PHI can sell for as much as $363 per record according to the Infosec Institute.

119. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

120. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

121. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.16 Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.

122. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

123. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

124. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

125. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

126. Medical information is especially valuable to identity thieves.

127. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.

128. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

129. For this reason, Defendant knew or should have known about these dangers and strengthened its network and data security systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

HARM TO PLAINTIFF

130. On or about March 25, 2022, Plaintiff Angulo received notice from Defendant that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's PHI, including name, address, date of birth, patient account number, diagnostic information, and claim information, was compromised as a result of the Data Breach.

131. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has spent several hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

132. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

133. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

134. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

135. This Action is properly maintainable as a Class Action. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Federal Rule of Civil Procedure 23, for the following Class and Subclass defined as:

National Class. All individuals and entities residing in the United States whose PII and PHI was compromised in the data breach first announced by Defendant in March of 2022.

California Subclass. All individuals and entities residing in California whose PII and PHI was compromised in the data breach first announced by Defendant in March of 2022.

136. Excluded from the Classes are: Defendant and Defendant's relatives, subsidiaries, affiliates, officers and directors, and any entity in which the Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

137. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

138. Numerosity. SCH reports that the Data Breach compromised PHI of 300,000 of patients. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

139. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner and

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages and/or injunctive relief.

140. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's PHI, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by SCH's uniform

conduct. Plaintiff are advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

141. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class in that they has no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel experienced in complex consumer class action litigation, including, but not limited to, similar data breach class action litigation, and Plaintiff intends to prosecute this action vigorously.

142. Superiority of Class Action. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set

of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

143. The litigation of the claims brought herein is manageable. SCH's uniform conduct, the consistent provisions of the relevant laws and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

144. Adequate notice can be given to Class members directly using information maintained in CIO's records.

145. Predominance. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

146. This proposed class action does not present any unique management difficulties.

V. CAUSES OF ACTION

FIRST CAUSE OF ACTION
Violation of the California
Confidentiality of Medical Information Act ("CMIA")
(On behalf of the California Subclass)

147. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

148. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

149. Defendant is a "contractor" within the meaning of Civil Code § 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

150. Plaintiff and all members of the Class are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiff and the Class fear that disclosure of their medical information could subject them to harassment or abuse.

151. Plaintiff and the respective Class members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the breach.

152. Defendant, through inadequate security, allowed unauthorized third-party access to Plaintiff's and each Class member's medical information, without the prior written authorization of Plaintiff and the Class members, as required by Civil Code § 56.10 of the CMIA.

153. In violation of Civil Code § 56.10(a), Defendant disclosed Plaintiff's and the Class members' medical information without first obtaining an authorization. Plaintiff's and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.10(a).

154. In violation of Civil Code § 56.10(e), Defendant further disclosed Plaintiff's and the Class members' medical information to persons or entities not engaged in providing direct health care services to Plaintiff or the Class members or their providers of health care or health care service plans or insurers or self-insured employers.

155. Defendant violated Civil Code § 56.101 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class.

156. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and the Class members' medical information in a manner that failed to preserve and breached the

confidentiality of the information contained therein. Plaintiff's and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

157. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and the Class members' medical information. Plaintiff's and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

158. Plaintiff's and the Class members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

159. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiff's and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

160. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class.

161. As a result of Defendant's above-described conduct, Plaintiff and the Class have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36.

162. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

163. Plaintiff, individually and for each member of the Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each Class

member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

SECOND CAUSE OF ACTION
Violations of California's Unfair Competition Law
(On behalf of the California Subclass)

164. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

165. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

166. In the course of conducting its business, Defendant committed "unlawful" business practices by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class members' PII, and by violating the statutory and common law alleged herein. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's

above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

167. Defendant also violated the UCL's unlawful prong by breaching contractual obligations created by its Privacy Policy and by knowingly and willfully or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of their posted privacy policy. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of their Privacy Policy.

168. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their Private Information. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their Private Information and identities.

169. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices

are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the California Consumer Privacy Act, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

170. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of its Privacy Policy and statutory and common law in that a portion of the money Plaintiff and Class members paid for Defendant's products and services went to fulfill the contractual obligations set forth in their Privacy Policy, including maintaining the security of their PII, and Defendant's legal obligations and Defendant failed to fulfill those obligations.

171. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

172. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately

caused the Data Breach and their violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property as a result of Defendant's unfair and deceptive conduct. Such injury includes paying for a certain level of security for their PII but receiving a lower level, paying more for Defendant's products and services than they otherwise would have had they known Defendant was not providing the reasonable security represented in their Privacy Policy and as in conformance with their legal obligations. Defendant's security practices have economic value in that reasonable security practices reduce the risk of theft of customer's PII.

173. Plaintiff and Class members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) deprivation of the value of their PII for which there is a well-established national and international market, and/or (iv) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

174. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class members, and the general public, also seek

restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

THIRD CAUSE OF ACTION
Brach of Implied Contract
(On behalf of the National Class or, alternatively, the California Subclass)

175. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

176. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

177. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

178. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

179. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

180. . Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

181. The protection of Plaintiff's and Class Members' Private Information was a material aspect of the implied contracts between Defendant and its patients.

182. The implied contracts – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

183. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the

implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

184. Consumers of medical services value their privacy and the ability to keep their Private Information associated with obtaining medical services private. To patients such as Plaintiff and Class Members, medical services that do not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than medical services that adheres to industry-standard data security.

185. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendants in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

186. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and paid for the provided medical services in exchange for, amongst other things, the protection of their Private Information.

187. Plaintiff and Class Members performed their obligations under the contract when they paid for their medical services and provided their valuable Private Information.

188. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendants gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Breach.

189. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notifications of the Breach to Plaintiff and thousands of Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

190. The Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

191. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received medical services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were

damaged in an amount at least equal to the difference in the value of the medical services with data security protection they paid for and the financial services they received.

192. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have received medical services from Defendant.

193. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

194. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Breach.

195. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH CAUSE OF ACTION
Negligence
(On behalf of the National Class or, alternatively, the California Subclass)

196. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

197. Defendant required Plaintiff and the Class Members to submit non-public personal information in order to obtain medical services.

198. The Class members are individuals who provided certain PII and PHI to Defendant including, but not limited to, their names, addresses, Social Security Numbers and/or Driver's License Number, and "medical information" as a necessary condition of SCH providing medical services to the Class members.

199. SCH had full knowledge of the sensitivity of the PII and PHI to which it was entrusted and the types of harm that Class members could and would suffer if the information were wrongfully disclosed.

200. SCH had a duty to each Class member to exercise reasonable care in holding, safeguarding and protecting that information.

201. Plaintiff and the Class members were the foreseeable victims of any inadequate safety and security practices.

202. The Class members had no ability to protect their data in SCH's possession.

203. By collecting and storing this data in its computer property, and by sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and the Class members' PII and PHI held within it—to prevent disclosure of the information and to safeguard the information from theft.

204. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

205. Defendant owed a duty of care to safeguard the PII and PHI of Plaintiff and Class members in its custody. This duty of care arises because Defendant knew of a foreseeable risk to the data security systems it used. Defendant knew of this foreseeable risk because of the explosion of ransomware and data breach incidents involving healthcare providers detailed above. Despite its knowledge of this foreseeable risk, Defendant failed to implement reasonable security measures.

206. Defendant owed a duty of care to Plaintiff and the Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII and PHI.

207. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as the common law.

208. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

209. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

210. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

211. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

212. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

213. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Class members' PHI and PII.

214. The specific negligent acts and omissions committed by Defendant SCH includes, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures to safeguard Class members' PII and PHI;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class members' PII and PHI;

e. Failing to detect in a timely manner that Class members' PII and PHI had been compromised;

f. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages and

g. Failing to have mitigation and back-up plans in place in the event of a cyber- attack and data breach.

215. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII and PHI would result in injury to Plaintiff and Class members.

216. Further, the breach of security was reasonably foreseeable given the known high frequency of hacking incidents, cyberattacks, and data breaches in the healthcare industry.

217. It was therefore foreseeable that the failure to adequately safeguard Class members' PII and PHI would result in one or more types of injuries to Class members.

218. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Breach.

219. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) provide adequate credit monitoring to all Class members.

VI. PRAYER FOR RELIEF

220. **WHEREFORE**, Plaintiff, individually and on behalf of the Class defined herein, prays for judgment as against Defendant SCH as follows:

a.) For an Order certifying this action as a Class action and appointing Plaintiff and their counsel to represent the Class;
b.) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class Members' PII and PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c.) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Breach;

d.) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e.) Ordering Defendant to pay for a lifetime of credit monitoring services for Plaintiff and the Class;

f.) For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law;

g.) For an award of punitive damages, as allowable by law;

h.) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i.) Pre- and post-judgment interest on any amounts awarded and,

j.) All such other and further relief as this court may deem just and proper.

JURY DEMAND

221. Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all claims in this Complaint so triable.

Dated: April 12, 2022

Respectfully submitted,

/s/ Alex Straus

Alex Straus (SBN 321366)

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

280 South Beverly Drive

Beverly Hills, California 90212

Tel.: (917) 471-1894

astraus@milberg.com

Attorneys for Plaintiff and the Classes